TILT LAW & TECHNOLOGY
WORKING PAPER SERIES

Criminal investigation and privacy in English law

Bryce C. Newell

Tilburg University, TILT
b.c.newell@tilburguniversity.edu

Version 1.0, February 2017

Citation: B.C. Newell, Criminal investigation and privacy in English law, TILT Law & Technology Working Paper Series, version 1.0, February 2017.

Abstract

The law regulating criminal investigation both legitimates the government's use of power and limits it by setting conditions for intrusions on fundamental rights and liberties. Privacy is one of the most prominent issues in establishing and limiting investigation powers. This paper analyses criminal investigation in relation to privacy in English law, with particular focus on privacy-related limitations and safeguards to criminal investigation powers. As part of a large-scale project on privacy protection in the 21st century, together with similar country studies, it will facilitate comparative legal analysis of criminal investigation (a relatively under-researched field), and also help to better understand privacy, as the forms and scope of privacy protection in criminal investigation law tell us something about how legislators conceptualize privacy, and how and to what extent the law protects different types of privacy.

Acknowledgements

This working paper has benefitted greatly from contributions by Sergi Vazquez Maymir. A substantial portion of the text below is based on his research and writing, as a research assistant in 2016. We are also grateful to Andrew Roberts, whose willingness to review and comment on this research-in-progress as it progresses has improved the results significantly.

Privacy-related crimes in English law

Version 1.0 (working paper), 28 February 2017

CONTENTS

1. Introduction

This report provides an overview of how privacy is protected through the law of criminal procedure in England and Wales. This working paper, which is part of a larger and on-going project, provides an overview of (selected) privacy-related aspects of English criminal procedure. We structure our analysis along four types of objects of the right to privacy, as identified in our earlier work: the protection of persons, places, things, and data.[1] Because the overall goal of this project is to generate a better understanding of the concept of privacy and its importance in our contemporary society filled with myriad new forms of surveillance and other privacy intrusions (and to do so from a comparative perspective), we conceptualize privacy broadly and include provisions that relate to the broad theme of protecting aspects of persons and their personal lives (encompassing the various types and dimensions of privacy we present in Koops, et al. (2017)). This conceptualization undoubtedly encompasses a large part of criminal procedure law. The current working version of this draft includes more substantive analysis of particular provisions (those prioritized by our on-going research to date), and additional analysis and analysis of additional provisions will continue to be added as the research progresses.

NOTE: we have not yet completely analyzed the impact of the adoption of the Investigatory Powers Act (IPA). That new legislation may well impact our analysis below, and updates will be reflected in subsequent changes to this working document.

Sections 2-3 outline criminal provisions related to protecting places (section 2), and persons (section 3).

2. The protection of places

2.1. The home

Public Authorities can gather information about that occurring inside people's homes either by entering the property, or by means of external observation. In both cases there is an interference with a private property and the collection of personal information. The legal grounds for bot activities are however different.

When the investigation involves an entry onto private premises or the interference with wireless telegraphy, this will require an authorisation, in the case of the intelligence services, under s. 5 of the Intelligence Services Act 1994[2] and in all other cases, under Part III of the Police Act 1997.[3] Differently, when the investigation involve the distant surveillance of that happening within the residential premises, the activities will be subject to Part II of Regulation of Investigation Powers Act 2000 (hereinafter "RIPA" or "the 2000 Act").

2.1.1. Surveillance

The definition of surveillance provided by S. 48(2) describes it as the "monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications, recording any of this". These surveillance activities shall be considered

[1] *See* Koops, et al., *A Typology of Privacy*, 38 U. PA. J. INT'L L. __ (2017) (forthcoming).
[2] S.5 Intelligence Service Act 1994: " No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section. Accesible at < http://www.legislation.gov.uk/ukpga/1994/13/section/5 >
[3] see s 48(3)(c) of RIPA accessible at< http://www.legislation.gov.uk/ukpga/2000/23/section/48 >

covert if, and only if, they are carried out in a manner calculated to ensure the actions go unnoticed for those how are under investigation.[4]

Part II of RIPA provides for the authorization of covert surveillance by public authorities where that surveillance is likely to result in the obtaining of private information about a person. At the same time, it provides the statutory framework under which covert surveillance activity can be conducted compatibly with the Human Rights Act 1998[5] (HRA). Similarly, an authorization under the 2000 Act is not required if a public authority has another clear legal basis for conducting covert surveillance likely to result in the obtaining of private information about a person. For example, the Police and Criminal Evidence Act 1984 provides a legal basis for the police covertly to record images of a suspect for the purposes of identification and obtaining certain evidence.[6]

2.1.2. Types of covert surveillance

Part II of the RIPA, distinguishes three types of covert surveillance: directed surveillance, intrusive surveillance, and covert human intelligence sources. Following the Covert surveillance and property interference code of practice (CSPI) [7], I will describe the two first, intrusive and directed:

Intrusive Surveillance

Section. 26 (3) RIPA defines Intrusive Surveillance, as the covert surveillance "carried out by an individual on residential premises or in any private vehicle or is carried out by a surveillance device in relation to anything taking place on residential premises or in a private vehicle."[8]

Whenever using surveillance technologies not situated in the premises or vehicle, s. 26(5) RIPA[9] adds that if the device is not actually present on the premises or in the vehicle the surveillance will not be regarded as intrusive unless the device is such that it consistently provides information of the same quality and detail.

It is thus possible for intrusive covert surveillance to take place by means of a device placed outside the premises or vehicle or place inasmuch it provides information of the same quality and detail as might be expected to be obtained from a device inside the premises.

> Example given by the CSPI: The observation outside residential premises providing a limited view compared to that which would be achievable from within the premises does not constitute intrusive surveillance. However, the use of a zoom lens, for example, which consistently achieves imagery of the same quality as that which would be visible from within the premises, would constitute intrusive surveillance.

The intrusiveness of investigatory conducts carried by public authorities are specifically excluded by S. 26 (4) to the extent that, a) they are carried out by means only of a surveillance device designed or adapted principally for the purpose of providing information about the

---

[4] **S. 26(9)(a) RIPA**< http://www.legislation.gov.uk/ukpga/2000/23/section/26 >

[5] The Human Rights acts gives effect in UK law to the rights set out in the European Convention of Hhuman Rights (ECHR). Art 8 ECHR describes the qualified right of a person to respect for his/her private and family life, home and correspondence.

[6] Covert Surveillance and Property Interference Code of Practice, NOTE:It seems that the code has been withdrawn on April 5, 2016, however there is no latter version published yet and in some sources (westlaw) appears as currently in force.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/514063/code-of-practice-covert.pdf

[7] supra

[8] S. 26 (3) RIPA accessible at < http://www.legislation.gov.uk/ukpga/2000/23/section/26 >

[9] http://www.legislation.gov.uk/ukpga/2000/23/section/26

location of a vehicle; or (b) it is surveillance consisting in any such interception of a communication as falls within section 48(4).[10]

Directed surveillance

Direct surveillance is essentially covert surveillance in places other than residential premises or private vehicles. It involves the covert monitoring of target's movements, conversations and other activities. According to s 26(2) directed surveillance is that that is" covert and undertaken for the purposes of a specific investigation, is likely to result in the obtaining of private information about a person (even though that person may not be specifically identified in relation to the operation), and is not an immediate response to circumstances or events"[11].

Authorization of directed surveillance is outlined in s. 28 and requires only internal authorization. A designated person may grant authorization for the carrying out of directed surveillance if he believes that it "is proportionate to what is sought to be achieved".

Consequently, covert surveillance of a specific person, where not intrusive (not residential premises nor private vehicle), would constitute directed surveillance if such surveillance is likely to result in the obtaining of private information about that, or any other person.

2.1.3. The concept of residential premises

For the purposes of RIPA, the limits of what is understood as a residential premise, is provided by s. 48(1), which describes it as:

> so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation, including hotel or prison accommodation that is so occupied or used.[12]

When considering the limits of such premises, s.48(7)(b),[13] specifically exclude those common areas to which a person has or is allowed access in connection with his use or occupation of any accommodation. RIPA further states (s.48.(8) that the concept of premises should be taken to include any place whatsoever, including any vehicle or moveable structure, whether or not occupied as land.

As a result, it seems that the residential premises ends circumscribed to the space where the owner or occupant can have exclusive access. Consequently, the front garden or driveway of premises readily visible to the public would not considered as a residential premise. Similarly, the communal stairway in a block of flats, would not fall within the notion of residential premise according to RIPA. On the other hand, the backyard of a house or a terrace when exclusively part of the property (the house), would positively qualify as such.

2.1.4. Considering home emanations

The definition of residential premises in combination with the types of covert surveillance provided by RIPA, sets a framework that focuses on the protection of places over people's

[10] References in this Part to surveillance include references to the interception of a communication in the course of its transmission by means of a postal service or telecommunication system if, and only if: (a)the communication is one sent by or intended for a person who has consented to the interception of communications sent by or to him; and
(b)there is no interception warrant authorising the interception.
[11] S.26 ( ) RIPA
[12] S. 48 (1) RIPA
[13] S. 48 (8.b) RIPA

expectations to privacy. On the other hand, the 2000 Act seems delineate the area of these premises restrictively and as a consequence so it does with the notion of intrusiveness.

Moreover, from the wording of s.26(5), it can be stated that the intrusiveness of the surveillance will, besides from the location of its target, rely on the capabilities of the devices used. As a result, a device placed in a public space to gather information from inside a residential premise, will be deemed intrusive depending on the quality of the information obtained, irrespective of the actual invasion of privacy derived from the investigatory activities.

The practical effect is that the capability of the equipment used will determine the extent of the authorisation required rather than the impact of the invasion of privacy. The blurred boundaries between direct and intrusive surveillance might represent the authorisation of the former made on the basis of wider grounds than intrusive surveillance, with only internal authorisation[14], though the effect on the individual's private life might be equally intrusive[15].

Examples

Listening within residential premises

The recording or monitoring of an individual's conversation within residential premises by a surveillance device as part of an authorized intrusive surveillance operation will not constitute interception under Part I of the 2000 Act[16] provided the process by which the product is obtained does not involve any modification of, or interference with, a telecommunications system or its operation. This will not constitute interception as sound waves obtained from the air are not in the course of transmission by means of a telecommunications system (which, in the case of a telephone conversation, should be taken to begin with the microphone and end with the speaker). Any such product can be treated as having been lawfully obtained.[17]

Noise investigations

The covert recording of suspected noise nuisance where the intention is only to record excessive noise levels and the recording device is calibrated [only to do that] does not require of an authorization according to RIPA. In such circumstances the perpetrator would normally be regarded as having forfeited any claim to privacy and an authorization may not be necessary.[18]

Sewage and wastewater[19]

Domestic waste is firstly carried by drains, a pipe that drains water and waste from a building and other buildings which belong with it (for example a garage).

The wastewater is later on carried by lateral drains, a length pipe which carries it away from the property. In this case, the pipe is located outside the property boundaries, often under a public pavement or road.

---

[14] See Annex: Authorizations procedures for directed and intrusive surveillance

[15] Akdeniz, Y.; Taylor, N.; Walker, C., Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State surveillance in the age of information and rights, [2001] Criminal Law Review, (February), pp. 73-90. Accessible at <http://www.leeds.ac.uk/law/staff/law6cw/clrrip06.pdf>

[16] The interception of communications sent by public post or by means of public telecommunications systems or private telecommunications is governed by Part I of the 2000 Act.

[17] Ibid 5

[18] Home Office CoP, para 2.29 accessible at <http://www.cieh.org/assets/0/72/998/1022/1046/1086/8b805d1c-f76d-46b6-bc7f-a589652409ab.pdf>

[19] Source: https://www.citizensadvice.org.uk/consumer/water/water-supply/sewerage/who-is-responsible-for-repairing-drains-and-sewers/.

Finally, the **s**ewer collects water and waste from the drains of a number of buildings. Most sewers are publicly owned and are maintained by a water company. However, there are still some privately owned sewers. Some people aren't connected to a sewer but to a cesspool**,** septic tank **or** treatment plant.

Now, when considering intrusiveness of the analysis by public authorities of the waste produced by a determined house, I am of the opinion, that whether such investigatory act would be understood as intrusive or directed surveillance, would be determined by the location where the device responsible of the analysis is placed.

Thus a surveillance device introduced in the house drains would, to the extent that they are inside the boundaries of the property, be considered as an act of intrusive surveillance. On the other hand, as soon as the device is located outside the residential premises, the surveillance would lose its intrusiveness and therefore considered directed.

2.1.5. **Directed video surveillance cameras at specific parts of homes**

The surveillance under RIPA seem to fail recognizing intrusiveness from investigations carried from outside the residential premises. This would for instance provide grounds to prolonged video surveillance of determined parts of home or areas place where the target would legitimately expect to enjoy privacy. Therefore, when considering the intrusiveness of the video recording of specific parts of the home, we should consider two elements:

Which part of the home is being recorded: s. 48(7)(b))[20] specifically excludes those common areas to which a person has or is allowed access in connection with his use or occupation of any accommodation. Thus the recording of the entrance of a house would for instance, not be considered intrusive and therefore would fall under directed surveillance.

The capacities of the recording device used: in order to be deemed intrusive the recording device should provide with information of a quality comparable to a device placed inside the premises.

2.2. Computers and other electronic devices

2.2.1. **Search and seizure of computers with a warrant**

The statutory criteria of a warrant are met, when the magistrates issuing it are provided with the necessary information to exercise their functions under section 8 of Police and Criminal Evidence Act 1984 (PACE).[21] Moreover, the warrant and its execution need to comply with the aspects set in both sections 15 and 16 on warrant safeguards together with the directions set out in Code B of the Codes of Practice.[22] Article 15 describes all the information that must be specified within the warrant in order to it to be lawful while art 16 defines the scope and limits of the constables while executing the warrant.

2.2.2. **Search and seizure of computers as main part of the investigation**

According to section 15 (6)(b) of PACE in relation to Search warrant safeguards, a warrant "shall identify, so far as is practicable, the articles or person to be sought." Considering the wording of s. 8(1) PACE, a warrant can embrace the identification of any material likely to be

[20] S. 48 (8.b) RIPA ibid
[21] Police and criminal Evidence Act, accessible at< http://www.legi1slation.gov.uk/ukpga/1984/60/section/8 >
[22] Accessible at< https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/306655/2013_PACE_Code_B.pdf >

relevant evidence.[23] It is important to note that the Serious Organised Crime and Police Act amended s. 8 of PACE to provide for warrants that cover multiple addresses and multiple entries at those addresses within a specified period. Post changes, warrants provide access to greater number of computers and devices and may be used on numerous occasions to locate and seize portable devices. Moreover, following s. 8(1.1C), a warrant may authorize multiple entries whenever the justice considers it necessary.

The terms "material" and "article" are not defined in PACE 1984.[24] The legislation was enacted before electronic storage of information—in computers, hard drives, mobile telephones, etc.—became ubiquitous, and the terms were more apt to describe things that could amount to evidence in themselves, rather than the evidence contained within them.[25] Important to note that the Serious Organised Crime and Police Act amended s.8 of PACE to provide for warrants that cover multiple addresses and multiple entries at those addresses within a specified period. Post changes – warrants provide access to greater number of computers and devices and may be used on numerous occasions to locate and seize portable devices.

Whilst it is clear that "material" is capable of including a computer, etc. and that a warrant that refers to "computer equipment" or similar may satisfy the requirements of PACE 1984 s. 15(6), the question of whether a warrant that authorizes a search for computers, computer equipment, hard drives, etc. satisfies that prescribed by s. 15(6) depends on the circumstances and, in particular, the nature of the investigation.[26]

Due to their characteristics, devices such as smart phones, computer hard drives or data sticks are likely to contain irrelevant material (mixed material) for an investigation, such as personal emails or photographs. The Court in Cabot Global Ltd v Barkingside Magistrates, affirmed (following previous rulings) that the existence of irrelevant material did not make the computer (or other devices) any less likely to be of substantial value to an investigation, as well as likely to be relevant evidence. Thus, the fact that devices containing relevant evidence were likely to contain irrelevant evidence too, "did not meant that a warrant [27]was improperly granted, as data stored on a computer was, for practical purposes, indivisible until it was examined and separated."[28]

When assessing whether a search under s.8 can be extended to other elements/items different from those identified in a warrant, the Courts agree to rely on the practicability[29] (within the meaning of section 15 (6) (b)) of specifying those other items. According to relevant case law,

---

[23] S8. PACE "In this Act *"relevant evidence"*, in relation to an offence, means anything that would be admissible in evidence at a trial for the offencae."

[24] Following the ruling in Cabot Global Ltd v Barkingside Magistrates': the word "material" in s.8 is capable of covering a computer and its hard disk.

[25] Legal analysis Cabot Global accessible at< http://login.westlaw.co.uk/maf/wluk/app/documentum%3Frank%3D1%26crumb- >

[26] See relevant jurisprudence below

[27] *"entry to search for, inter alia, "computer equipment, mobile phones … and cash representing the proceeds of criminal activity" did not breach the requirement in s.15(6)(b) that the warrant "identify, so far as is practicable, the articles … sought*"

[28] Reffering to *R. (on the application of Rabiul Hoque and Mridul Kanti Das) v City of London Police and The Commissioners of HM Revenue and Customs* (2013) EWHC 725 (Admin).

[29] Cabot Global Conclusion R (Glenn & Co (Essex) Ltd and others) v HM Commissioners for Revenue and Customs and another (2011) EWHC 2998 (Admin); (2012) 1 CR App R 22 " *the question of where the balance lines in an individual case will not be answered by reference to authority, since each case is likely to turn on particular facts. It will be answered by considering whether the warrant has identified the articles sought "so far as practicable" in the circumstances".*

it can be stated, that Courts are rather permissive when it comes to interpreting the scope of the search and seizure of computers and similar devices.

Relevant Case Law

In *McGrath v. Chief Constable of the Royal Ulster Constabulary [2001]* in the context of an arrest warrant, the court determined that a warrant should be sufficiently clear and precise for those interested in their execution to know precisely what are the limits of the power.

Kent Pharmaceuticals Ltd v. Serious Fraud Office [2002]The broad scope of an investigation may require a correspondingly broad power of search, and make it less 'practicable' (to use the word in section 15(2)(b) and (6)(b)) to identify the articles sought.

In *R (Faisaltex Ltd) v Preston Crown Court and others [2008]*: The Divisional Court observed that Section 8(1) of PACE refers to "material" which is likely to be relevant evidence, and "material" clearly has a wide meaning under that statute. It was concluded that the word "material" could itself cover a computer and, for that matter, its hard disk.

In R *v Inland Revenue Commissioners* [30] the court rejected an analogy with a filing cabinet, which suggested that a hard disk is simply a "container of files visible to the computer's operating system … . "If there is incriminating (in the normal sense of the word) material on the hard disk, and if it is assumed that the hard disk is not copied, the computer itself may be used, and may be required, as evidence in order to prove the existence of the incriminating material on the defendant's computer. The fact that there is also on the hard disk material that is irrelevant, and not evidence of anything, does not make the computer any less of a thing that may be required as evidence for the purposes of criminal proceedings."

In *R v Revenue and Customs Commissioners* [31] it was suggested the tension between the requirements that a warrant be sufficiently clear and precise by declaring that

> for those interested in their execution to know precisely what are the limits of the power" and the difficulty of drafting a warrant in the context of a broad and/or complex investigation: "the question of where the balance lies in an individual case will not be answered by reference to authority, since each case is likely to turn on particular facts. It will be answered by considering whether the warrant has identified the articles sought 'so far as practicable' in the circumstances

In *R (on the application of Rabiul Hoque and Mridul Kanti Das) v City of London Police and The Commissioners of HM Revenue and Customs (2013):* The claimants' second ground of claim is that no justice of the peace could properly have concluded that "mobile telephone communications, including handsets, SIM cards, computer processing equipment, including portable storage records and media records" were likely to have been "relevant evidence" for the purpose of section 8(1)(c) and (iv) of the Act. This court has recognised in R(Faisaltex Ltd) v Preston Crown Court & Anor [2009] 1 WLR 1689 (Admin) that computers, if likely to contain relevant evidence, are likely also to contain evidence not relevant to an investigation. That does not mean that the constable enforcing the warrant is bound only to seize that which is relevant, since data stored on a computer is for practical purposes indivisible until it is examined and separated. The claimants contend that HMRC was not required by the justices during the application for the warrant to justify its application to recover electronic material, and it follows that the issue of relevance was not properly addressed. I do not accept these contentions. It seems to me to be obvious from the contents of the information that the HMRC

---

[30] Accessible at < *R. (on the application of H) v Inland Revenue Commissioners [2002] EWHC 2164 (Admin); [2002] S.T.C. 1354*>

[31] *R. (on the application of Glenn & Co (Essex) Ltd) v Revenue and Customs Commissioners [2011] EWHC 2998 (Admin); [2012] 1 Cr. App. R. 22* (p.291),

investigation embraced not only the business records of the claimants and their companies but also communications between the claimants themselves and between the claimants respectively and their senior employees. HMRC had cause to believe that the claimants were not merely acting coincidentally in their efforts to cheat the Revenue but were acting in concert. That being the case, computer and telephone equipment was likely to reveal the association between the two men and the coordination of their activities. I do not consider for these reasons that ground 2 is made out.

In Cabot Global Ltd v Barkingside Magistrates(2015): if there are reasonable grounds to believe that there is incriminating material on the computer, tablet, smart telephone or similar device, then it may constitute relevant evidence, thereby properly forming the subject of an order under section 8 Police and Criminal Evidence Act 1984 . The fact that there may also be material that is irrelevant does not make the computer any less "*material* " which is likely to be of substantial value to the investigation, as well as likely to be relevant evidence.

2.2.3. **Warrantless search and seizure**

Officers are empowered to carry searches without a warrant in determined situations by virtue of s.17, 18 and 32 of PACE (searches following incident to lawful arrest). Section 32 provides an important search power. Under that section, when a person is arrested at a place other than a police station, the provision enables police to search the person, the premises where he is arrested or where he was immediately prior to arrest for evidence of an offence. If someone is arrested for almost any offence it might enable portable devices to be seized and searched for evidence (e.g. in the case of a mobile phone to enable location analysis to be carried out, etc.).

According to ss. 17 and 18, police can enter a premises if they need to stop a crime in progress, prevent a crime that they suspect is about to occur, enforce an arrest warrant, or recapture a person unlawfully at large. Thus, police can raid a property without a search warrant and without anyone's consent if there is an arrest warrant issued by a magistrate and police officers have reasonable grounds to believe an individual is on the property. If the subject in question is already under arrest for a causes that may eventually lead to a trial, police can enter and search his/her home, without a warrant and without consent if there is a reasonable ground for suspecting they may find evidence, about the offence that lead to the arrest or for any other offence.[32] This power also applies to any property occupied or controlled by the subject or any premises the subject is in at the time of the arrest or immediately before it.

2.2.4. **Search of electronic devices found during a broader search of a person or place**

During a search, police officers may encounter electronic devices for which they have reasonable grounds to believe there is relevant evidence for the investigation. A distinction should be made here between the power to search and that one to seize. [33]While searching shall remain on the originating ground allowing the search (either warrant or legal power) , the seize of the "new" devices might be carried through sections 19 and 20 PACE or by means of section 50ss of the Criminal Justice and Police Act 2001 (CJPA).

[32] But see section 32, the power to search premises that are not the 'controlled or occupied' by the arrestee.
[33] Sections 19 and 20 of the Police and Criminal Evidence Act 1984 and section 50 Criminal Justice and Police Act 2001 are concerned not with powers of search but instead with powers of seizure. See Cabot.

Section 19(1) of PACE enables a constable to seize items where they are lawfully on the premises, and s. 19(4)12 provides the constable with powers in relation to data in digital format:[34]

> The constable may require any information which is stored in any electronic form and is accessible from the premises **to be produced in a form in which it can be taken away** and which it is visible and legible or from which it can readily be produced in a visible and legible form if he has reasonable grounds for believing
>
> > (a) that- (i) it is evidence in relation to an offence which he is investigating or any other offence; or (ii) it has been obtained in the commission of an offence; and (b) that it is necessary to do so in order to prevent it being concealed, lost, tampered with, or destroyed.

Section 20 extends the power to a constable carrying a search to:

> (..) require any information [stored in any electronic form] and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible [or from which it can readily be produced in a visible and legible form. (…)

Section 50 CJPA on the other hand, enables a person already authorized to search and seize to remove an item to determine whether it falls within the seizure power. It does not render the seizure of computers or mobile telephones under s.8 of the 1984 Act unlawful, the additional power of seizure from premises under s.50 does not invalidate the taking of devices under a warrant issued under s. 8 if there are reasonable grounds for believing that they may contain relevant evidence.

Finally section 51 CJPA[35] also provides for similar, additional, powers of seizure from a person where existing powers already exist to carry out a search of the person. Paragraph 165 of the Explanatory Notes [36]explain the need for this additional provision:

> This section gives additional powers of seizure from the person where there is an existing power to search that person. It is almost identical to section 50. It is necessary because, for example, individuals might have on them handheld computers or computer disks which might contain items of electronic data which the police would wish to seize. Alternatively, they could be carrying a suitcase containing a bulk of correspondence which could not be examined in the street.

Besides, the classic procurement of information via copy of determined files, these provisions cover the use of imaging technology, that is, to obtain copies of data held on a computer, as accepted in the case of *Paul Da Costa & Co v Thames Magistrates Court*[37] where images of hard drives were taken by Customs during a search.[38]

---

[34] Stephen Mason, Esther George Digital evidence and cloud computing (2011): *Stone observes that this might include data held anywhere in the world[34], and the practical problems relating to this becomes obvious for a constable, who may be exposed to a civil action for trespass against items that were seized and later shown to be exempt from seizure*

[35] Additional powers from seizure from the person < accessible at <http://www.legislation.gov.uk/ukpga/2001/16/section/51>

[36] Explanatory Notes CJPA 2001 <accessible at http://origin-www.legislation.gov.uk/cy/ukpga/2001/16/notes >

[37] The Queen on the Application of Paul Da Costa & Co (A Firm) and Stewart Collins v Thames Magistrates Court and H.M. Commissioners of Customs & Excise , CO/3157/2001 , later applied in Burgin v Commissioner of Police of the Metropolis (2011)

[38] in respect of Commissioners of the Inland Revenue, see R (on the application of H) v Commissioners of Inland Revenue [2002] EWHC 2164 (Admin).

As mentioned above, whether is proportionate to seize and retain the devices or its enough with a copy/procure of the same, it is something that needs to be assessed case by case[39].

The degree of protection available to those who are the subject of a search involving computer equipment or similar varies depending on the power under which Act/ power the equipment is seized.[40]Where it is not possible to separate the relevant material from the irrelevant material at the scene, the Criminal Justice and Police Act 2001 (CJPA) establishes an important procedure to ensure the sifting, separation, protection and return of irrelevant material to the owner as soon as possible.

Where 'mixed material' is seized, police are obliged to serve a notice under section 52 of the CJPA on the person from whom property has been seized. The service of the notice triggers a 'sifting' process designed to identify, separate out and return irrelevant material as soon as practicable. Section 53 of CJPA confirms an entitlement on the owner of the property or their legal representative to be present while the sifting exercise takes place in order to safeguard their private interests. A failure to follow this process amounts to a breach of the CJPA and the right to privacy, enshrined in Article 8 of the European Convention on Human Rights and the common law.[41]

2.3. Digital searching of computers

In the case of a physical crime, police might need to execute a search warrant at the suspect's home to gather sufficient proof that the suspect committed the crime. In the digital version of the crime, a search warrant is likely to be essential. Thus what has been described in previous sections, apply here as well.

Moreover, in order to prevent those subject to a computer search alleged officers have imported or altered data, the Association of Chief Police Officers has a Good Practice Guide (ACPO) to meet the challenges of contamination. It isn't law nor is it a statutory Code of Practice, but breach will result in the drawing of adverse inferences. Section1 of ACPO[42] set the four principles to be followed by the relevant authorities when conducting searches related to computers or similar devices.

> Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.
>
> Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions
>
> Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
>
> Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to

---

[39] In Cabot, the Court considered the possibility of seizing the "relevant material" within computers in paper form or on memory sticks to be unrealistic and impractical, due to the amount of data contained in these devices and the immense length of time to identify any relevant documents from those that are not.

[40] supra

[41] The limits of intrusion: your rights in relation to search warrants issued under the Terrorism Act accessible at< http://cage.ngo/uncategorized/limits-intrusion-your-rights-relation-search-warrants-issued-under-terrorism-act/>

[42] http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Arguably, these principles list police management's primary concerns with the execution of digital search and seizure procedures. These are (1) the willful changing of data; (2) the competence of the examiners to assess relevance; (3) the ability of examiners to generate an audit trail; (4) and certain unspecified concerns with adequately following the law.[43]

Although failure to adhere to these guidelines will not necessarily render the data obtained as being inadmissible, nevertheless the police will need to explain to a judge why they did not follow the guidelines in circumstances where the guidelines could not be followed. There are times when it will be impossible to follow the guidelines fully, especially when the police have to obtain copies of complex live banking systems, for instance. The practical consequences of taking a forensically sound copy of the data are that the police have a range of copies of the data: the "original" or master, which is, in effect, the actual device (if a device is seized); a copy for back-up purposes, and a working copy for the police to interrogate without affecting the data that was originally seized.[44]

3. The protection of persons

3.1. Protections for behavioural privacy

3.1.1. Location tracking

In England and Wales, the Regulation of Investigatory Powers Act (RIPA)[45] is the primary piece of legislation that regulates location tracking by law enforcement. However, certain forms of location tracking may also fall within the scope of two other pieces of legislation. First, the Intelligence Services Act 1994 applies to surveillance conducted by the British intelligence services (e.g., Secret Intelligence Service, Government Communications Headquarters). Second, the Police Act 1997 applies to surveillance that would interfere with property or wireless telegraphy (including physical or non-physical trespass). Thus, location tracking could potentially require authorisation under RIPA as well as additional authorisations under one or both of these additional laws. The Home Office has promulgated a number of codes of practice, including for Covert Surveillance and Property Interference[46] (regulating the conduct of public authorities) and Equipment Interference[47] (regulating the intelligence services). Because the police and the intelligence services are regulated somewhat separately, it is important to distinguish which Act and associated codes of practice apply in any given situation.

To engage in location tracking or other forms of surveillance, the police must obtain an "authorisation" whenever the intended surveillance is "directed" or "intrusive," as defined by RIPA s. 26. Authorisations, which typically last for three months, do not generally need to be

[43] Gary Lilienthal, Nehaluddin Ahmad The digital age meets the law of search and seizure: an overview of US, UK and Europe scenarios.
[44] Esther George and Stephen Mason. Obtaining evidence from mobile devices and the cloud (2015)
[45] Regulation of Investigatory Powers Act 2000, c. 20 (2000).
[46] Home Office (UK), Covert Surveillance and Property Interference: Code of Practice: Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000, December 2014. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384975/Covert_Surveillance_Property_Interrefernce_web__2_.pdf.
[47] Home Office (UK), Equipment Interference: Code of Practice: Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000, January 2016. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/496069/53693_CoP_Equipment_Interference_Accessible.pdf.

judicially approved, as a designated official of a public body (e.g., an appointee within the police services) may execute authorisations. For most police forces, this will be the Superintendent.[48] An authorisation for "directed surveillance" or "intrusive surveillance" under RIPA (Part II) provides a public authority with "a lawful basis (…) to carry out covert surveillance activity that is likely to result in the obtaining of private information about a person."[49] Private information is defined as "any information" that relates to the "private or family life" of any person.[50]

Authorisations for covert surveillance are appropriate only when the surveillance is intended to fulfil one or more statutorily defined purposes (including preventing or detecting crime or protecting national security), and the authorized surveillance should be proportionate to the purpose it aims to achieve and be carried out as part of a specific investigation or operation.[51] The Code of Practice stipulates that the following proportionality elements should be taken into account:

> balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
>
> explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
>
> considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
>
> evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented. [52]

Section 3.21 of the Covert Surveillance Code of Practice states that

> police applications for directed (…) surveillance (…) must only be made by a member or officer of the same force as the authorising officer, unless the Chief Officers of the forces in question have made a collaboration agreement under the Police Act 1996 and the collaboration agreement permits applicants and authorising officers to be from different forces.[53]

Because the UK is signatory to the European Convention on Human Rights (ECHR), decisions of the European Court of Human Rights (ECtHR) are also relevant to location tracking by British police. The ECtHR has held that GPS surveillance is less intrusive, in terms of violations of Article 8 of the ECHR, than

> other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings.[54]

However, as indicated by the Home Office in its code of practice (cited above), various forms of covert surveillance, when combined with other methods of investigation, may capture private personal information, even when the form of surveillance by itself would not.

---

[48] The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, Schedule 1. The prescribed authorizing officer depends on the particular police force (military police for example has different positions/ranks). *See* 2010 Order (footnote 40), Schedule 1.
[49] Home Office, Covert Surveillance Code of Practice, *supra* note 46 at 26.
[50] Regulation of Investigatory Powers Act 2010 § 26(10).
[51] Regulation of Investigatory Powers Act 2010 §§ 28(3), 28(4).
[52] Home Office, Covert Surveillance Code of Practice, *supra* note 46 at 27.
[53] Covert Surveillance and Property Interference Code of Practice, p. 31
[54] Uzun v. Germany ECHR (2010) 35623/05

The legal goods (interests) protected

The surveillance-related provisions in Part II of RIPA are primarily intended to restrict or regulate law enforcement efforts to obtain *private information* about a person by means of covert surveillance activities—as well as related police interference with property and communication (via wireless telegraphy). The Act extends to "monitoring, observing or listening to persons, their movements, conversations or other activities and communications."[55]

Types of location tracking

Visual observation

Visual observation, whether accomplished by the unaided eye or through the use of video surveillance cameras, is subject to RIPA's authorisation requirements only when it is covert and carried out as part of a specific investigation into a person or group of persons (i.e., thus the meaning of "directed" surveillance). As defined in RIPA,

> surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place.

Visual surveillance, even if covert, is not subject to RIPA when it is conducted as part of general observation activities (e.g., an undercover officer out on patrol, investigatory activities designed to detect crime rather than to investigate a particular person) and in immediate response to events (i.e. emergencies or other situations where obtaining an authorisation is unpractical), among other situations.[56] However, when covert visual surveillance is used as part of a targeted investigation of a particular person or group of persons, RIPA requires the police to obtain appropriate approval. Additionally, overt use of CCTV and automatic number plate recognition (ANPR) cameras is not subject to RIPA.

GPS or other tracking devices

Location tracking is directed surveillance, under RIPA, when it is done covertly and is likely to obtain private information about an individual. Intrusive surveillance, which is subject to heightened regulation, is covert surveillance that is "carried out in relation to anything taking place on any residential premises or in any private vehicle" and that involves the use of a surveillance device or physical trespass into a residential premises or vehicle).[57] However, otherwise intrusive surveillance that only involves the use of a surveillance device designed or adapted solely to provide information about the location of a vehicle (and does not involve physical trespass) is not considered intrusive.[58] The relevant code of practice also presumes that such use of a surveillance device, on its own, may not always constitute directed surveillance, as it may not result in capturing private information about an individual.[59] As such, the limited use of such a tracking device by itself (e.g., to determine the location of a vehicle at one given point in time) may not be subject to regulation at all (if its use is not likely to obtain private information about any individual). However, when the use of the device (including when it is used in conjunction with other forms of investigatory activities) is likely to result in capturing private information (e.g., "monitoring … the movements of the

---

[55] Home Office, Covert Surveillance Code of Practice, *supra* note 46 at 7.
[56] Home Office, Covert Surveillance Code of Practice, *supra* note 46 at 18-25.
[57] Regulation of Investigatory Powers Act 2000 § 26(3).
[58] Regulation of Investigatory Powers Act 2000 § 26(4).
[59] Home Office, Covert Surveillance Code of Practice, *supra* note 46 at 14 ("The use of surveillance devices designed or adapted for the purpose of providing information regarding the location of a vehicle alone does not necessarily constitute directed surveillance as they do not necessarily provide private information about any individual but sometimes only supply information about the location of that particular device at any one time.").

occupant(s) of [a] vehicle"), the surveillance must be authorized as a form of directed surveillance under RIPA.[60] If the use or installation of the device also encompasses an interference with property, a separate authorization under the Police Act 1997 may also be required. To further complicate the analysis, if location tracking is accomplished by means that also result in the interception of communications, the police must also obtain an interception warrant under Part I of RIPA. RIPA, s. 26(2)(c) also exempts covert surveillance carried out in "immediate response" to events where obtaining an authorization unpractical.

Many forms of location tracking require deployment of specialized equipment—e.g., GPS-devices—in advance. Such activities will constitute property interference (if it concerns a device that is independently attached to property, e.g., a vehicle, and sends back location-data to the police) or, in the case of the intelligence services, equipment interference (if the device actively interferes with other electronic equipment in order to achieve the desired result). It is also conceivable that police could track someone's location through remote interference without actually placing a device (e.g. hacking into a smartphone) which would then constitute directed surveillance (if done by the police) but not property interference or, if carried out by the intelligence services, such conduct might potentially constitute equipment interference. It is equally conceivable that police would be able to track someone's location through intercepting their communications; this would then require an interception warrant.

3.2. Police hacking powers and the interception of communications

The Investigatory Powers Act (IPA), also known as the Snooper's charter, was recently passed by parliament and received Royal Assent on the 29th of November 2016. In addition to consolidating and clarifying existing powers, it also adds several new powers (some of which are quite invasive compared to anything available up to this point). Not surprisingly, the bill was quite controversial and received a considerable amount of criticism. Regardless of what one's opinion may be, it is clear the legal landscape surrounding police hacking powers has changed significantly with enactment of IPA. An overview of the relevant legislation is in order.

There is little academic literature available that gives a clear overview of police hacking powers in the UK. The most useful reference point is an article by Sommer which outlines the available technologies and their respective legal contexts.[61] While useful, the article is significantly outdated. Fortunately, the various codes of conduct released in conjunction with enactment of the relevant legislation provide additional clarity. [62][63]

The focus here is primarily on police hacking powers, although some attention has been paid to intelligence agencies as well.

3.2.1. **Computer Misuse Act 1990**

The Computer Misuse Act 1990 (CMA) criminalizes activities relating to computer misuse. In the original version, only section 1(1) (unauthorized access to computer material) was covered

[60] Home Office, Covert Surveillance Code of Practice, *supra* note 46 at 18.
[61] Sommer, Peter. "Police Powers to Hack: Current UK Law." *Computer and Telecommunications Law Review* 18.6 (2012): 165. http://www.pmsommer.com/Police%20Powers%20to%20hack.pdf
[62] Equipment Interference DRAFT Code of Practice https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557861/IP_Bill_-_Draft_EI_code_of_practice.pdf
[63] Interception of Communications DRAFT Code of Practice https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/561091/16-10-18_Interception_code_of_practice_draft.pdf

under a law enforcement exception. The CMA also dealt with other computer-related offenses (such as impairment) for which, originally, no law enforcement exceptions were enacted. This legal discrepancy was noted by Sommer, who wrote his article before the amendment by the Serious Crimes Act 2015.[64] Through this act, the CMA itself was expanded upon by adding more types of computer misuse offences. In conjunction, Section 10, which deals with law enforcement exceptions, was also expanded upon and now also applies to sections 2 (unauthorized access with intent to commit or facilitate commission of further offences), 3 (unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.), 3ZA (unauthorized acts causing, or creating risk of, serious damage) and 3A (making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA). The legal discrepancy previously mentioned has thus been solved.

It is interesting to note that the CBA amendment from the Serious Crimes Act 2015 received a great deal of criticism. The UK government was accused of 'changing the law under the radar', in an attempt to avoid 'proper debate'. [65] Others have argued that the amendment did not fundamentally change anything in that it merely consolidates and clarified already existing powers. Indeed, the Guardian quotes a Home Office spokesperson as saying that *"there have been no changes made to the Computer Misuse Act 1990 by the Serious Crime Act 2015 that increase or expand the ability of the intelligence agencies to carry out lawful cybercrime investigation."*.[66] I am inclined to follow the latter explanation, as the CMA merely deals with the question whether certain acts of computer misuse constitute a criminal offense, exempting law enforcement where necessary. It does not explicitly regulate specific powers (other than referring to standard police powers of inspection, search and seizure). It is clear that other acts address a wide variety of powers which extend beyond the original scope of the CMA (many types of police hacking will constitute more than merely 'unauthorized access to computer material' and incorporate elements of impairment). In that sense, the CMA has merely been updated to accurately reflect reality and bring things in line with other legislation (although this does technically mean that some hacking acts by the police have been illegal in the past) and pave the way for IPA.

In essence, the key feature of the CMA is that it *'provides that access will not be 'unauthorized' and an offence will not be committed if the conduct in question takes place pursuant to a relevant authorization*'.[67] We must therefore look towards other legislation from which such authorizations can originate.

3.2.2. **Traditional inspection, search and seizure**

The Police and Criminal Evidence Act 1984 (PACE) grants police powers of inspection, search and seizure. All powers of seizure are extended to include computerized information.[68] Officers may demand log-in information from users in order to be able to access the computer.[69] The CMA explicitly accounts for and exempts conduct based on these powers from unlawfulness.

---

[64] Sommer, Peter. "Police Powers to Hack: Current UK Law." *Computer and Telecommunications Law Review* 18.6 (2012): 165. p. 7

[65] Drinkwater, Doug. "GCHQ and police hackers protected by revised Computer Misuse Act" https://www.scmagazineuk.com/update-gchq-and-police-hackers-protected-by-revised-computer-misuse-act/article/537065/

[66] Bowcott, Owen. "Intelligence officers given immunity from hacking laws, tribunal told" https://www.theguardian.com/uk-news/2015/may/15/intelligence-officers-have-immunity-from-hacking-laws-tribunal-told

[67] Equipment Interference DRAFT Code of Practice, 2.25, p. 12

[68] Police and Criminal Evidence Act 1984

[69] Police and Criminal Evidence Act 1984, section 20

These powers form the basics of police 'hacking powers' but are mainly relevant for the classic situation where police physically search a premises under authority of a warrant and confiscate evidence. I will therefore turn my attention to more recent forms of legislation that regulate more 'modern' forms of hacking, namely equipment interference and interception of communications.

3.2.3. **Equipment and property interference**

'Equipment interference' is only loosely defined in IPA itself, the code of practice however is more clear:

> Equipment interference describes a range of techniques used by the equipment interference agencies that may be used to obtain communications, equipment data or other information from the equipment. Equipment interference can be carried out either remotely or by physically interacting with the equipment. Equipment interference operations vary in complexity (...) More complex equipment interference operations may involve exploiting existing vulnerabilities in software in order to gain control of devices or networks to remotely extract material or monitor the user of the device.[70]

Thus, in order for something to be 'equipment interference' under IPA, the purpose must be the obtaining of communications, equipment data or other information from the equipment. A warrant is required if the act of equipment interference would (otherwise) constitute a criminal offense under the CMA. As opposed to warrants dealing with interception of communications (which only the Secretary of State may issue for law enforcement), warrants for equipment interference can be issued by a law enforcement chief. [71] Equipment interference must be necessary for the purpose of preventing or detecting serious crime, preventing death or injury or (mitigating) any damage to a person's physical or mental health. Serious crime is defined as

> the offence, or one of the offences, which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age of 18 (or, in relation to Scotland or Northern Ireland, 21) and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more.[72]

It must also be proportionate to its intended purpose: law enforcement chiefs in particular, when issuing warrants, must take notice of several additional proportionality requirements, such as whether the appropriate law enforcement officer has the necessary expertise and training in order to conduct the equipment interference technique properly.[73] Additionally, there must also be satisfactory safeguards in place.[74] These safeguards *'relate to the copying, dissemination and retention of material'*.[75] Warrants may be issued urgently under certain circumstances, that is, without initial approval from a judicial commissioner.[76] Warrants issued urgently are valid for five working days (unless renewed by a judicial commissioner), as opposed to six months when issued through the standard procedure. Warrants may be renewed for six months.[77] Modifying warrants is also possible, but modifications must also be approved by a judicial commissioner.[78] If there is a clear link between acts of surveillance and the *'communications, equipment data or other information obtained from the equipment*

---

[70] Equipment Interference DRAFT Code of Practice, p. 8
[71] Ibid, p. 7
[72] Investigatory Powers Act 2016, section 263
[73] Equipment Interference DRAFT Code of Practice, p. 35
[74] Equipment Interference DRAFT Code of Practice, p. 33-34
[75] Ibid, p. 34
[76] Ibid, p. 37-39
[77] Ibid, p.40
[78] Ibid, p.41

interference', the surveillance will not require a separate authorization and will be covered under the equipment interference warrant.[79] Combined warrants may be issued for authorizations to interfere with property or authorization of surveillance (that is, surveillance without a link to the equipment interference). Sommer mentions the example of the physical key logger, a device which intercepts input as it travels from the keyboard to the computer. The device is placed and later retrieved. An equipment interference warrant under IPA provides the legal basis for covert installation of such a device.[80] Sommer considers the output of such a device 'direct surveillance' under the Regulation of Investigatory Powers Act 2000 (RIPA) and thus states that two types of authorization would be required. However, in the new legal landscape, a single authorization under IPA would most likely be enough: the surveillance is clearly 'linked' to the equipment interference, and through that surveillance the information is ultimately obtained.

If acts of equipment interference can be authorized under another law enforcement power (the code of practice mentions the example of '*a law enforcement officer interfering with equipment by seizing it pursuant to a warrant issued under the Police and Criminal Evidence Act 1984 (...).*', acquiring a warrant for equipment interference under IPA is not necessary.[81] It should be noted, however, that law enforcement may no longer rely on 'property interference authorizations' as they appear in the Police Act of 1997 Act when interfering with equipment for the goal of obtaining communications, private information or equipment data.[82] In that particular context, law enforcement must rely on a targeted equipment interference order (again, unless any other act than the 1997 Act is applicable).

Under IPA, intelligence agencies may also obtain 'bulk equipment interference warrants', which allows them to interfere with equipment on a large (international) scale. It *'collects data relating to a number of devices (for example, devices in a particular area) in order to identify potential targets of interest'*.[83] The Intelligence and Security Committee voices critique as to the fact that targeted warrants can also be used for bulk purposes, quoting the GCHQ Director who himself made this suggestion, stating that *"the dividing line between a large-scale targeted EI and bulk is not an exact one".*[84] Thus, in a sense, bulk equipment interference is equally available to law enforcement agencies, due to the fact that targeted equipment interference can be used in a similar manner.

Despite not being explicitly mentioned in the legislation itself, it clearly follows from the equipment interference code of conduct that intended intrusion, hacking innocent people who are not themselves the target of interest (but may nevertheless provide relevant information) is allowed.[8586] In the same vein, it is very likely that intended intrusion would also arise during

---

[79] Ibid, p.20

[80] Sommer, Peter. "Police Powers to Hack: Current UK Law." *Computer and Telecommunications Law Review* 18.6 (2012): 165. p. 7-8 / Note: Sommer actually names the Police Act of 1997 as a legal basis (property interference), but as will become clear, this is no longer allowed.

[81] Equipment Interference DRAFT Code of Practice, p.13

[82] Ibid, p.13

[83] Factsheet – Bulk Equipment Interference
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473753/Factsheet-Bulk_Equipment_Interference.pdf

[84] Intelligence and Security Committee of Parliament, 'Report on the draft Investigatory Powers Bill', p. 5
http://www.statewatch.org/news/2016/feb/uk-ics-rep-9-feb-16-surveillance.pdf

[85] Factsheet – Equipment interference
https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Equipment-Interference.pdf

[86] Note to Bryce: I am not 100 % sure that intended intrusion is also allowed for law enforcement agencies. The factsheet referenced above specifically names 'intelligence agencies' but the code of conduct speaks of

bulk equipment interference, as the chance (depending on the amount of devices or users) that the interference would only concern actual suspects or perpetrators seems very slim.

Generally speaking, equipment interference warrants granted under IPA are the go-to approach when conducting equipment interference for the purpose of obtaining communications, private information or equipment data. As previously mentioned, the 1997 Police Act provides for property interference (authorization of action in respect of property), but has been partly replaced since enactment of IPA. Nevertheless, there are plenty of situations where interference with equipment may be necessary for purposes other than obtaining communications, private information or equipment data. Law enforcement may hack a security system in order to disable it, but this does not constitute 'equipment interference' in terms of IPA, but rather 'property interference', and the 1997 Police Act will be the appropriate legislation to act under.

3.2.4. **Interception of communications**

The 'interception of communications' refers to any communication, including e-mails. In the same vein as the CMA, IPA criminalizes the act of intercepting communications, but provides exemptions for law enforcement if they have an interception warrant. As with equipment interference, proportionality, necessity, sufficient safeguards and judicial commissioner approval are required.[87] Warrants may be issued without (initial) judicial commissioner approval in case of urgency.[88] Interception warrants are valid for 6 months and may be renewed for another 6 months.[89] Warrants are not necessary in case consent is given by both recipient and sender, or by either recipient or sender (the latter situation will require an authorization for surveillance under RIPA, however).[90]

IPA discerns between targeted interception warrants (must specify a particular person, premises or operation) and bulk interception warrants.[91] The latter is not available to law enforcement, but allows intelligence agencies to intercept communications on a massive scale in a simultaneous manner.[92] Obtaining metadata (called 'secondary data' in IPA) is also possible through an interception warrant, be it targeted or bulk. Metadata can be the sole reason underpinning a warrant or it can be done in addition to the content of a communication.[93]

Warrants for targeted interception of communications are granted by the Secretary of State, and may be combined with warrants for targeted equipment interference, property interference and surveillance. [94]

3.2.5. **Conclusion**

While IPA has definitely simplified the legal framework surrounding police hacking powers by consolidating and clarifying existing powers, it has also expanded upon those powers significantly. As is clear, the legal framework is at significant odds with privacy. The legality of certain aspects of IPA (data retention) have already been called into question by the ECHR

'equipment interference agencies', which, as I understand it, can mean any potential agency using the powers described there, be it law enforcement or intelligence agencies or otherwise.

[87] Interception of Communications DRAFT Code of Practice, p. 11

[88] Ibid, p. 34

[89] Ibid, p. 35-36

[90] Investigatory Powers Act 2016, section 44

[91] Ibid, part 2 & 6 respectively.

[92] Ibid, section 130

[93] Interception of Communications DRAFT Code of Practice, p. 10

[94] Interception of Communications DRAFT Code of Practice, p. 25

in a very recent ruling.[95] In my opinion, a further and closer look at the ways in which several issues arising from IPA's enactment (such as intended intrusion, and the thin line between targeted and bulk equipment interference) relate to privacy rights could be very interesting.

3.3. Stop and search (in general)

Stop and search powers enable the police to investigate whether persons have committed, are committing or are about to commit a criminal offence. In England & Wales, the powers to stop and search persons, vehicles and others are provided for in general powers at common law, the most important powers are under Police and Evidence Act 1984 (PACE) , the Misuse of Drugs Act 1971, s. 23 and the Criminal Justice and Public Order Act 1994, s.60 (CJPOA), all in consonance with the codes of practice that regulate the powers of police in securing law and order in UK. There is generally no power to stop a person simply to question them, and there is no power to stop a person to find grounds for a search.[96]

3.3.1. **PACE**

Section 1 of PACE allows a constable to detain a person or a vehicle for the purpose of a search, and may seize the articles. The power can be exercised in a public when he has reasonable grounds for suspecting that as a result of the same, he might find stolen or prohibited articles[97]. A constable can only search a person in a yard or garden of a dwelling if he has reasonable grounds for believing that the person does not reside there and is not there with permission. There are similar restrictions on the search of a vehicle.

The test of reasonable suspicion is based on the facts and circumstances of a particular case.[98] Guidance as to what constitutes the objective test of reasonable suspicion is given in Code A of PACE in paras 2.2-2.11:[99]

> 2.2 Reasonable grounds for suspicion depend on the circumstances in each case. There must be an objective basis for that suspicion based on facts, information, and/ or intelligence which are relevant to the likelihood of finding an article of a certain kind or, in the case of searches under section 43 of the Terrorism Act 2000, to the likelihood that the person is a terrorist (…)
>
> 2.3 Reasonable suspicion may also exist without specific information or intelligence and on the basis of the behaviour of a person. For example, if an officer encounters someone on the street at night who is obviously trying to hide something, the officer may (depending on the other surrounding circumstances) base such suspicion on the fact that this kind of behaviour is often linked to stolen or prohibited articles being carried. Similarly, for the purposes of section 43 of the Terrorism Act 2000, suspicion that a person is a terrorist may arise from the person's behaviour at or near a location which has been identified as a potential target for terrorists.

Most importantly Code A states that suspicion should not be based on generalisations or stereotypes, but should be linked to accurate and current intelligence or information. The Code prohibits searches with consent of the subject if there is no legal power to search (para.1.5).

---

[95] Martin, Alexander. 'Landmark EU ruling: Legality of UK's Investigatory Powers Act challenged' http://www.theregister.co.uk/2016/12/21/eu_judgment/

[96] Kiron Reid (University of Liverpool). Stop and search

[97] Prohibited articles s.1(7) PACE include offensive weapons or articles made or adapted for use in connection with various offences

[98] Clark, D 2004, Bevan and Lidstone's The Investigation of Crime: A Guide to the Law of Criminal Investigation, Butterworths, London

[99] See also the Revised Code A 2014 accessible at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/392796/2014_PACE_Code_A_Revised__HOC__08-12-14.pdf >

The Codes of Practice are revised regularly. The most recent edition should be referred to. Police officers use the "GOWISELY" acronym to remember the information that they must give to the subject prior to stop and search.

In regard to searches incident to lawful arrest s.32[100] also allows the constable to search an arrested person at a place other than a police station if he/she has reasonable grounds for believing that the arrested person may represent a danger to himself or others. In practice this leads to an arrest enabling portable devices to be seized and searched for evidence under little basis, e.g. in the case of a mobile phone it might enable location analysis to be carried out. However, in the event that a mobile phone is protected by password, the search does not include per se, the power to request the password of the same. Section 49 of Pt III of RIPA states that a notice must be issued to the arrested person, containing certain prescribed information (see section 49(4) of the act). More importantly, the notice can only be given by an officer of at least the rank of superintendent (or an assistant chief constable where the search power used was section 44 Terrorism Act 2000) or someone acting with his/her permission. It is very unlikely that these requirements could be met in the course of a street search.

Safeguards[101]

Safeguards on use of the power are set out in ss.2 and 3. The constable must give their name and police station; the object of the search and the grounds for the search. If the constable completes a search of an unattended vehicle they should leave a notice with details. A person or vehicle can be detained for a reasonable amount of time (s.2(8)) but Code A makes clear this should be kept to a minimum (para.3.3). A search in public can only require the removal of outer coat, jacket and gloves. A more thorough search should be done out of public view. Only a constable in uniform can stop a vehicle. If a constable fails to take reasonable steps to comply with s.2 the search is unlawful (Sobczak v DPP [2012] EWHC 1319 (Admin); (2012) 176 J.P. 575). Failure to comply with the safeguards can lead to significant damages against the police. E.g. Browne v Commissioner of Police of the Metropolis [2014] EWHC 3999 (QB) for injury. Section 3 sets out provisions on record keeping. These have been contentious and have been changed several times in response to political and police lobbying. A record shall be made of a search unless it is not practicable to do so. This should include the ethnic origin of the person searched. Records have largely been seen as important to counter racial discrimination, but should also be used by police forces to review the legality and effectiveness of stop and search as a policing tool. The person searched is entitled to a copy of the record if they request one within three months. Following the Crime and Security Act 2010 s.1 there is no requirement to record the name, address and date of birth of the person searched, which limits the information available for scrutiny of the use of stop and search. This limits the effectiveness of monitoring and scrutiny which is encouraged by Pt 5 of Code A. Use of powers must comply with the Equality Act 2010 and the Children Act 2004.

3.3.2. The Misuse of Drugs Act 1971

This power has the same basis in principle as s.1 PACE, regarding possession of a controlled drug. Most searches across the UK are made for drugs. Black (Michael David) v DPP [1995] C.O.D. 381 held that B visiting a known drug dealer (his brother) was not sufficient to constitute reasonable grounds for suspicion that he was in possession of drugs. A difficulty for officers that the individual constable must have factual basis for suspicion is illustrated by the Scottish case, HM Advocate v B [2013] HCJ 71 (undercover officer who observed drugs being

[100] http://www.legislation.gov.uk/ukpga/1984/60/section/32
[101] Ibid 22

passed over instructing uniformed officer to search van insufficient). There is a power to search for firearms under s.47 of the Firearms Act 1968.

3.3.3. **CJPOA**

Under s.60, an officer of the rank of inspector may authorise stop and search without reasonable suspicion, in a defined area for a limited period if they reasonably believe that incidents involving serious violence may take place and it is expedient to use the powers to prevent them. The time period is up to 24 hours, which can be extended for a further 24 hours. Section 60AA of the CJPOA allows a constable to require the removal of face coverings used to conceal identity. Authorisation by an inspector is required. For the criteria see s.60AA. "Best Use of Stop and Search", below, encourages reduced use of s.60, partly through tighter authorisation criteria. However these have not been put in statute or statutory guidance. "Since a peak of 150,000 searches in the year ending March 2009, the use of section 60 stop and search has drastically declined". Police Powers and Procedures (2015, para.4.6). Much of the peak use was in the course of government encouraged action against knife crime.

Besides the already mentioned, there are other Acts empowering a constable to perform a stop and search:[102]

Section 2 of the Poaching Prevention Act 1862

Section 12 of the Deer Act 1991

Section 4 of the Conservation of Seals Act 1970

Section 11 of the Protection of Badgers Act 1992

Section 6 of the Public Stores Act 1875

Section 163 of the Customs and Excise Management Act 1979

Section 24B of the Aviation Security Act 1982

Section 27 (2) of the Aviation Security Act 1982

Section 7 of the Sporting Events (Control of Alcohol etc.) Act 1985

Section 34B of the Environmental Protection Act 1990

Section 47 of the Firearms Act 1968

Section 4 of the Crossbows Act 1987

Section 139B of the Criminal Justice Act 1988

Schedule 4 Paragraph 2A [25] of the Police Reform Act 2002

Section 43 of the Terrorism Act 2000

Section 47A of the Terrorism Act 2000

3.3.4. **Relevant case law**

R. (on the application of Roberts) v Commissioner of Police of the Metropolis: The power given to police under the Criminal Justice and Public Order Act 1994 s.60 to stop and search people or vehicles for offensive weapons was compatible with ECHR art.5 and art.8. The safeguards surrounding the use of the power, such as the requirement to

[102] Wikipedia via StopWatch accessible at< http://www.stop-watch.org/our-work/research-policy >

give reasons for the search and for the s.60 authorisation, made it possible to judge whether the power had been exercised lawfully.

*Colon v Netherlands ECtHR (2012)***:** The designation of parts of a city as security risk areas in which police could stop and search people at random for weapons did not violate the European Convention on Human Rights 1950 art.8 or Protocol 4 art.2.

3.4. Search and seizure and the terrorist threat

3.4.1. **Search and seizure**

Section 1 (1) and (2) of the Terrorism Act 2001 (TACT)[103] define "terrorism" as (i) the use or threat of action which (ii) (relevantly for the present case) "endangers a person's life, other than that of the person committing the action" where (iii) the use of threat is designed to influence the government or an international governmental organisation or to intimidate the public or a section of the public and (iv) the use or threat is made for the purpose of advancing a political, religious, racial or ideological cause.

The Broadness of the definition was discussed by the Supreme Court in the case of *R v Gul [2014] AC 1260, [2013] UKSC 64*, para 29:

> With great respect, the bare proposition that the definition of terrorism in section 1 is very wide or far reaching does not of itself instruct us very deeply in the proper use of Schedule 7 . There are however particular aspects which seem to me to be important for the ascertainment of the reach of the Schedule. First, section 1 does not create a criminal offence. The Act creates a separate regime of criminal offences: section 54 ff. That being so, we should not assume that foundational concepts of the criminal law, such as intention and recklessness, are to be read into provisions such as section 1(2)(c) ("endangers a person's life") or 1(2)(d) ("creates a serious risk to the health or safety of the public").Section 1(2) is concerned only to define the categories of "action" whose use or threat may constitute terrorism: not to impose any accompanying mental element. Similarly, the expression "concerned in" in section 40(1)(b) is not to be taken to import the criteria for guilt as a secondary party which the criminal law requires in a case of joint enterprise."

Schedule 5 of TACT, empowers magistrates to authorise police to enter and search specified premises and to confiscate personal property. An unduly broad or vague TACT search warrant may be susceptible to a legal challenge.

The power granted by Schedule 5(1) of TACT only allows authorities to seize "relevant material", which is likely to be of substantial value to a terrorist investigation. Again, as it has already mentioned above, following the relevant provisions in PACE, Police are required to give '*full and frank'* disclosure to the court when applying for a warrant and to identify, so far as practicable, the articles or persons sought . That means clearly setting out the evidential basis for a reasonable suspicion that identified items are likely to be found on the premises and are likely to be of substantial value to a terrorist investigation.[104]

---

[103]S1. TC2001 accsessible at< http://login.westlaw.co.uk/maf/wluk/app/document?src=doc&linktype=ref&context=98&crumb-action=replace&docguid=ID281F5E0E45011DA8D70A0E70A78ED65 > ; See also How UK's terrorism law targets words, not just guns and bombs . The Guardian accessible at < https://www.theguardian.com/law/2014/jul/22/terrorism-law-targets-words-guns-bombs >

[104] The limits of intrusion: your rights in relation to search warrants issued under the Terrorism Act accessible at< http://cage.ngo/uncategorized/limits-intrusion-your-rights-relation-search-warrants-issued-under-terrorism-act/ >

Both the police and the magistrate can be obliged to disclose to the occupier a copy of the information laid before the magistrate leading to the grant of the warrant. Requesting disclosure of the application for the warrant can be an important mechanism for checking that the police and the magistrate have adhered to the necessary legal requirements.

3.4.2. **Stop and search**[105]

The Terrorism Act 2000, in its Section 43(1) provides a power for a constable to stop and search a person whom he or she reasonably suspects [106]is a terrorist, to discover whether that person has anything in their possession which may constitute evidence they are a terrorist. ." Section 43A applies similarly to vehicles. Anti-terrorism powers are wider than the standard powers in regard to stop and search (Terrorism Act 2000 as amended by the Protection of Freedoms Act 2012).

Moreover, section 43(2) also provides a power for a constable to search a person arrested under section 41 of that Act to discover whether that person has anything in their possession which may constitute evidence they are a terrorist. In contraposition to PACE, 43(2) does not require prior reasonable suspicion that such evidence may be found.

The power to search someone under section 43[107] of the TACT, which depends on an officer having reasonable suspicion that the person he/she intends to search is involved in terrorism, extends to looking for "anything which may constitute evidence that [the person being searched] is a terrorist."[108]

Section 44 powers[109]—for which an officer does not need reasonable suspicion because a designation covering a specific area is in place— extends to searching for "articles of a kind

---

[105] The text in this section does not yet account for possible changes that made by the Protection of Freedoms Act 2012 (Chapter 2 Part 4), or the modifications to the legislation made by statutory the instrument entitled The Terrorism Act 2000 (Remedial) Order 2011 SI 2011/631.

[106] Reasonable grounds for suspicion depend on the circumstances in each case. There must be an objective basis for the suspicion (that the person is a terrorist or that the vehicle is being used for the purposes of terrorism) based on relevant facts, information, and/ or intelligence. Reasonable suspicion must rely on intelligence or information about, or behaviour by, the person or vehicle concerned. Unless the police have a description of a suspect, a person's physical appearance (including any of the "protected characteristics" set out in the Equality Act 2010), cannot be used alone or in combination with each other or with any other factor, as the reason for searching that person. Reasonable suspicion cannot be based on generalisations or stereotypical images of certain groups or categories of people as more likely to be involved in terrorist activity.

[107] S.43 TACT : Search of persons.

1)A constable may stop and search a person whom he reasonably suspects to be a terrorist to discover whether he has in his possession anything which may constitute evidence that he is a terrorist.
(2)A constable may search a person arrested under section 41 to discover whether he has in his possession anything which may constitute evidence that he is a terrorist.
(3)A search of a person under this section must be carried out by someone of the same sex.
(4)A constable may seize and retain anything which he discovers in the course of a search of a person under subsection (1) or (2) and which he reasonably suspects may constitute evidence that the person is a terrorist.
(5)A person who has the powers of a constable in one Part of the United Kingdom may exercise a power under this section in any Part of the United Kingdom.

[108] https://www.theguardian.com/commentisfree/libertycentral/2009/aug/04/liberty-clinic-stop-search-mobile

[109] Provision 44. Authorisations.

(1)An authorisation under this subsection authorises any constable in uniform to stop a vehicle in an area or at a place specified in the authorisation and to search—
(a)the vehicle;
(b)the driver of the vehicle;
(c)a passenger in the vehicle;
(d)anything in or on the vehicle or carried by the driver or a passenger.

which might be used in connection with terrorism." This definition may be wide enough to allow officers to look through the contents of a person's phone.[110]

Section 47A allows searches in specified areas or places without reasonable suspicion to find evidence related to terrorism. This must be authorised by a senior officer who reasonably suspects that an act of terrorism will take place, and reasonably considers that the authorisation is necessary. This replaced the provisions in s.44 which were found in breach of art.8 ECHR in Gillan v United Kingdom (4158/05) (2010) 50 E.H.R.R. 45.

The s.44 powers were widely criticised for being deployed mostly but ineffectively against ethnic minorities after the terrorist attacks in New York on 11 September 2001. They were also used against peaceful protesters. For examples see Race issues and stop and search: looking behind the statistics J. Crim. L. 2009, 73(2), 165-183 at pp.174-175. In the House of Lords in Gillan, Lord Bingham erroneously argued that the then powers "cannot, realistically, be interpreted as a warrant to stop and search people who are obviously not terrorist suspects, which would be futile and time-wasting." (para.35). This assertion is incorrect as that is exactly a point of blanket powers - that anyone can be stopped. It can be argued that the deterrent and usefulness is made more useful because it is hard to identify who are suspected terrorists. The House of Lords had upheld the lawfulness of the suspicionless stop power. (CF Roberts, SC para.41, which contradicts earlier approval of this passage). The Terrorism Act powers are subject to a Code of Practice under that Act. Code A PACE includes some guidance on use of powers in Sch.5 to the Terrorism Prevention and Investigation Measures Act 2011, which do not require reasonable suspicion by a constable. Para. 2.18A.

3.4.3. **Searches at ports and border controls**

Schedule 7 to the Terrorism Act 2000 empowers "examining officers" (constables, immigration officers and customs officers) to stop, question, search, and detain persons at ports or borders. The powers apply whether or not the examining officer has grounds to suspect that person of being a terrorist (para. 2(4))[111]. It is an offence to fail wilfully to comply with an examining officer's request.[112]

The power, has been given to provide an opportunity for the ascertainment of the *possibility* that a traveler at a port may be concerned in the commission, preparation or instigation of an act of terrorism[113]

In *Bank Mellat v Her Majesty's Treasury* the proportionality of the measure was addressed in its para 20:

---

(2)An authorisation under this subsection authorises any constable in uniform to stop a pedestrian in an area or at a place specified in the authorisation and to search—
(a) the pedestrian;
(b) anything carried by him.
(3)An authorisation under subsection (1) or (2) may be given only if the person giving it considers it expedient for the prevention of acts of terrorism.

[110] Ibid 23 / (** powers to search on designated areas cheek)

[111] paragraph 2(4) of Schedule 7 establishess that an examining officer is not required to have any "grounds for suspecting that a person falls within section 40(1)(b) ". Nor does Schedule 7 provide that an examining officer must be the one to determine whether the subject appears to fall within that subsection. It may well be someone else, to whom the results of the stop are referred.
The s.44 powers were widely criticised for being deployed mostly but ineffectively against ethnic minorities after the terrorist attacks in New York on 11 September 2001.

[112] Shona Wilson Stsark. Suspicion-less minds: anti-terrorism powers at ports and borders. Cambridge Law Journal

[113] Para 58 Miranda

> … [T]he question depends on an exacting analysis of the factual case advanced in defence of the measure, in order to determine (i) whether its objective is sufficiently important to justify the limitation of a fundamental right; (ii) whether it is rationally connected to that objective; (iii) whether a less intrusive measure could have been used; and (iv) whether, having regard to these matters and the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.

In assessment of the proportionality of a decision to exercise the stop power is fact-sensitive. It is necessary to have regard to the interests of the person who is to be stopped on the basis of the facts as they were or ought to have been known to those who exercised the power. Against those interests there must be weighed (on the facts of this case) the national security interests of the community.[114]

Paragraph 2(5) of Schedule 7 provides that a person who is questioned under para 2 must "(a) give the examining officer any information in his possession which the officer requires". Moreover, para 18 provides that a person commits an offence punishable with a sentence of imprisonment and/or a fine if he "(a) wilfully fails to comply with a duty imposed under or by virtue of this Schedule". On the other hand, the only sanction for disobedience to an explanation order made under para 13 of Schedule 5.

There are constraints on the exercise of the power that he held to amount to adequate safeguards. These are (i) the requirements of the general law that the power be exercised on a reasoned basis, proportionately and in good faith; (ii) the limitation on the meaning of terrorism given by reference to the mental or purposive elements prescribed by section 1(1)(b) and (c) of TACT ; (iii) the fact that the power may only be exercised "at a port or in the border area"; and (iv) the fact that the power of detention is limited to nine hours.

Relevant Case Law

Miranda v. Secretary of State (2016): The power conferred by the Terrorism Act 2000 Sch.7 para.2(1) to stop and question a person at a port or border area was incompatible with ECHR art.10 in relation to journalistic material, in that it was not subject to adequate safeguards against its arbitrary exercise.

Gillan v United Kingdom: Police powers under anti-terrorism legislation that authorised, and provided a wide discretion to execute, the stop and search of individuals in public without the need for reasonable suspicion of wrongdoing were neither sufficiently circumscribed nor subject to adequate legal safeguards against abuse, and violated the European Convention on Human Rights 1950 art.8.

Beghal v DPP: the power in the Terrorism Act 2000 Sch.7 to question and search at ports and borders was not incompatible with ECHR art.8.

[114] Miranda para 61